IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

MAGIC LABS, INC.,)
)
Plaintiff,)
)
v.) C.A. No. 23-967 (RGA)
)
HORKOS, INC. d/b/a PRIVY)
)
Defendant.)

DEFENDANT HORKOS, INC.'S OPENING BRIEF IN SUPPORT OF MOTION TO DISMISS COMPLAINT PURSUANT TO FED. R. CIV. P. 12(B)(6) AND 35 U.S.C. § 101

MORRIS, NICHOLS, ARSHT & TUNNELL LLP
Jack B. Blumenfeld (#1014)
Brian P. Egan (#6227)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
jblumenfeld@morrisnichols.com
began@morrisnichols.com

Attorneys for Defendant

OF COUNSEL:

Clement S. Roberts
ORRICK, HERRINGTON
& SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

Alyssa Caridis
ORRICK, HERRINGTON
& SUTCLIFFE LLP
355 South Grand Avenue, Suite 2700
Los Angeles, CA 90071
(213) 629-2020

November 16, 2023

TABLE OF CONTENTS

Page

I. NATURE AND STAGE OF THE PROCEEDING 1

II. SUMMARY OF ARGUMENT 1

III. STATEMENT OF FACTS 1

A. Cryptographic Keys 2

B. The ’321 Patent 3

IV. LEGAL STANDARD 5

V. ARGUMENT 6

A. *Alice* Step One: The Representative Claim Is Directed To An Abstract Idea. 6

1. Software Facilitation Of A Known Process Is An Abstract Idea 7

2. The Claim Merely Recites Generic Data Transmission And Manipulation. 9

3. The Claim Is Not Directed To An Improvement In Computer Functionality. 10

B. *Alice* Step Two: The Claim Includes No Inventive Concept 14

C. The Remaining Claims Are Similarly Ineligible. 18

VI. CONCLUSION 20

TABLE OF AUTHORITIES

Page(s)

Cases

Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.,
728 F.3d 1336 (Fed. Cir. 2013)....................16

Affinity Labs of Tex., LLC v. DirectTV, LLC,
838 F.3d 1253 (Fed. Cir. 2016)....................5, 10

Alice Corp. Pty. Ltd. v. CLS Bank Int'l,
573 U.S. 208 (2014).................... *passim*

Apple, Inc. v. Ameranth, Inc.,
842 F.3d 1229 (Fed. Cir. 2016)....................11

Asghari-Kamrani v. United Servs. Auto. Ass'n,
No. 15-cv-478, 2016 WL 3670804 (E.D. Va. July 5, 2016), *aff'd*, 737 F. App'x 542 (Fed. Cir. 2018) 16

Ashcroft v. Iqbal,
556 U.S. 662 (2009)....................5

Bancorp Servs., LLC v. Sun Life Assur. Co. of Can.,
687 F.3d 1266 (Fed. Cir. 2012)....................19

BASCOM Glob. Internet Servs. v. AT&T Mobility LLC,
827 F.3d 1341 (Fed. Cir. 2016)....................17, 18

Boom! Payments, Inc. v. Stripe, Inc.,
839 F. App'x 528 (Fed. Cir. 2021) 13

Broadsoft, Inc. v. CallWave Commc'ns, LLC,
282 F. Supp. 3d 771 (D. Del. 2017)....................8

buySAFE, Inc. v. Google, Inc.,
765 F.3d 1350 (Fed. Cir. 2014)....................20

Card Verification Solutions, LLC v. Citigroup Inc.,
No. 13 C 6339, 2014 WL 4922524 (N.D. Ill. Sept. 29, 2014)....................8

ChargePoint, Inc. v. SemaConnect, Inc.,
920 F.3d 759 (Fed. Cir. 2019)....................6, 12

Cloud Satchel, LLC v. Amazon.com, Inc.,
76 F. Supp. 3d 553 (D. Del. 2014)....................8

Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.,
776 F.3d 1343 (Fed. Cir. 2014)....................3, 5

Credit Acceptance Corp. v. Westlake Servs.,
859 F.3d 1044 (Fed. Cir. 2017)....................6

Customedia Techs., LLC v. Dish Network Corp.,
951 F.3d 1359 (Fed. Cir. 2020)....................11, 13

Elec. Power Grp., LLC v. Alstom S.A.,
830 F.3d 1350 (Fed. Cir. 2016)....................9, 11

EveryMD.com LLC v. Amazon.com, Inc.,
No. CV-17-05573, 2017 WL 6886181 (C.D. Cal. Dec. 5, 2017), *aff'd*, 737 F. App'x 538 (Fed. Cir. 2018) 8

Fast 101 Pty Ltd. v. Citigroup Inc.,
424 F. Supp. 3d 385 (D. Del. 2020)....................20

Free Stream Media Corp. v. Alphonso Inc.,
996 F.3d 1355 (Fed. Cir. 2021)....................12

GeoComply Sols. v. Xpoint Servs.,
No. 22-1273, 2023 WL 1927393 (D. Del. Feb. 10, 2023)....................14

GoDaddy.com LLC v. RPost Commc'ns Ltd.,
No. CV-14-00126, 2016 WL 3165536 (D. Ariz. June 7, 2016), *aff'd*, 685 F. App'x 992 (Fed. Cir. 2017) 8

In re TLI Commc'ns LLC Patent Litig.,
823 F.3d 607 (Fed. Cir. 2016)....................11, 15, 17

Intellectual Ventures I LLC v. Erie Indem. Co.,
850 F.3d 1315 (Fed. Cir. 2017)....................14, 19

LendingTree, LLC v. Zillow, Inc.,
656 F. App'x 991 (Fed. Cir. 2016) 8

Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.,
566 U.S. 66 (2012)....................5

Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.,
811 F.3d 1314 (Fed. Cir. 2016)....................14

Prism Techs. LLC v. T-Mobile USA, Inc.,
696 F. App'x 1014 (Fed. Cir. 2017) 11

Rady v. Boston Consulting Grp.,
20-cv-02285, 2022 WL 976877 (S.D.N.Y. Mar. 31, 2022)....12

RecogniCorp, LLC v. Nintendo Company,
855 F.3d 1322 (Fed. Cir. 2017)....9

Secured Mail Sols. LLC v. Universal Wilde, Inc.,
873 F.3d 905 (Fed. Cir. 2017)....5

Smart Sys. Innovations, LLC v. Chi. Transit Auth., Cubic Corp.,
873 F.3d 1364 (Fed. Cir. 2017)....10

Synopsys, Inc. v. Mentor Graphics Corp.,
839 F.3d 1138 (Fed. Cir. 2016)....16

Trading Techs. Int'l, Inc. v. IBG, LLC,
921 F.3d 1378 (Fed. Cir. 2019)....14

Universal Secure Registry LLC v. Apple Inc.,
10 F.4th 1342 (Fed. Cir. 2021) .... *passim*

I. NATURE AND STAGE OF THE PROCEEDING

Magic Labs, Inc. ("Magic") alleges that Horkos, Inc. d/b/a Privy ("Privy") infringes U.S. Patent No. 11,546,321 ("the '321 patent"), which claims software that facilitates the process of an end user setting up storage of digital "keys" with a third-party key storage provider.

II. SUMMARY OF ARGUMENT

Patent law does not protect abstract ideas, even when a patent claims those ideas in a particular technological context. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 223 (2014) (providing framework for determining subject matter eligibility under § 101). It is well established that using software to facilitate storing valuables with a third-party intermediary is an abstract idea. *See, e.g.*, *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1350 (Fed. Cir. 2021). Indeed, using software to implement and facilitate a third-party storage system was the exact idea the Supreme Court found to be abstract and patent-ineligible in *Alice*. 573 U.S. at 223. The claims of the '321 patent are directed to the very same abstract idea.

The claims of the '321 patent contain no technological innovation to transform this abstract idea into a patent-eligible invention. Instead, the claims call only for conventional data transmission and manipulation steps, performed using generic computer components. And while Magic alleges that the '321 patent claims embody an inventive "architecture," that *conclusion* is belied by the plain language of the claims and Magic's admissions about what was in the prior art.

III. STATEMENT OF FACTS

Magic and Privy are software companies that develop systems for creating and maintaining blockchain[1] wallets. D.I. 1 ¶¶ 6, 8, 15. Magic owns the '321 patent, titled "Non-Custodial Tool

[1] A "blockchain" is a distributed "ledger" of transactions—a public list with identical copies on computers across the world—that can track the ownership and exchange of digital assets, such as cryptocurrency. D.I. 1 ¶¶ 8–9. Though this case involves technology used to build blockchain-

for Building Decentralized Computer Applications." '321 patent, Title. The patent purports to disclose "an improved system for securing data" that involves having users generate a cryptographic key and then having users send the key to a third-party key storage provider. *Id.* at 1:41, 12:8–12; *see also id.* at 1:51–55; D.I. 1 ¶ 30. On September 1, 2023, Magic sued Privy, alleging infringement of at least claim 11 of the '321 patent. D.I. 1 ¶¶ 36–61. Privy now moves to dismiss.

A. Cryptographic Keys

The '321 specification explains that the "username/email/phone+password security model" relied on by many web-based applications provides subpar security. '321 patent, 1:8–15, 3:27–32. This is because "password leaks are prevalent," and hackers are proficient at using leaked passwords to compromise accounts. *Id.* at 1:11–15, 3:29–32.

Cryptographic keys are a longstanding security tool that are used (as inputs to a cryptographic algorithm) to encrypt and decrypt information. *See* D.I. 1 ¶ 23 (cryptographic "key systems existed long before [blockchain technology]"). Cryptographic keys may include a public/private key pair: information is encrypted using a "public key" and can only be decrypted by the corresponding "private key," which must be kept secret. *See id.* at ¶¶ 22–23. In the blockchain context, public-private key pairs can be used to transfer and prove ownership of digital assets. *Id.* But cryptographic keys are difficult to manage because, *e.g.*: they are long and random, they cannot be changed, and private keys must be kept secret. '321 patent, 3:34–40; D.I. 1 ¶ 24.

Prior to the '321 patent, there were well-known solutions for an end user to "manag[e], control[], and us[e] cryptographic keys." D.I. 1 ¶¶ 24–29. As described by Magic, one such well-known solution involved an end user generating keys locally and then sending them to a third-

based computer applications, the patent claims are largely independent from blockchain technology.

party provider that stores and encrypts the keys "on a [hardware security module ("HSM")] operated in a secure cloud environment." *Id.* ¶ 27. This "third-party HSM[]" sits between the user and an application that requires the use of the keys, much like an escrow service. *Id.*

The problem with this approach, according to Magic, was that the end user bore the burden of "generating keys and coordinating with the third-party provider," and third-party HSMs were "complicated and expensive to set up." *Id.*; '321 patent, 3:34–36 ("[C]onsumer deployment of cryptography-based security has failed to provide an acceptable user experience."). This was the problem that the '321 patent was intended to address.

B. <u>The '321 Patent</u>

The '321 patent seeks to provide a secure and convenient way for end users to generate and store cryptographic keys. It purports to improve on the prior art by providing a "non-custodial" method for generating cryptographic keys and sending them to a third-party key storage provider. '321 patent, 1:51–55. The system is "non-custodial" because the software implementing the method never has access to the generated keys. *Id.*; D.I. 1 ¶¶ 30–31. Instead, a key "is created on a client machine" and then sent directly to a third-party key storage provider for storage and encryption. '321 patent, 1:51–55.

Claim 11—the only claim mentioned in Magic's complaint and representative of the '321 patent claims[2]—recites the following:

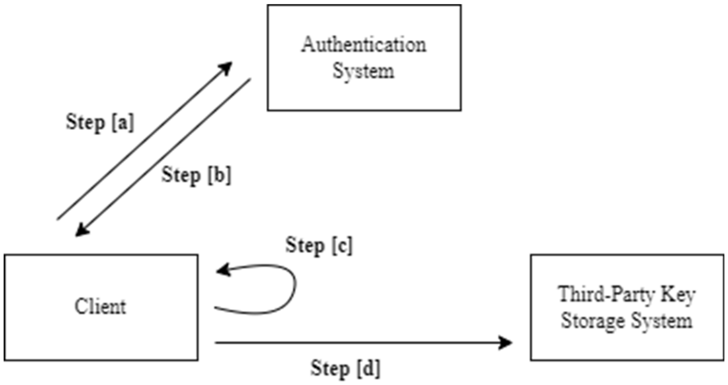
[2] Claim 11 is representative because all the claims of the '321 patent "are substantially similar and linked to the same abstract idea." *Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.*, 776 F.3d 1343, 1348 (Fed. Cir. 2014). Nonetheless, this motion also addresses the remaining claims. *See infra* 18–20.

11. A non-transitory computer readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method to setup a wallet for a decentralized application by performing a non-custodial authentication method for a client, the method comprising:

> **[a]** *sending*, over a network by the client to an authentication system, a sign-up request for a user account associated with the decentralized application;
>
> **[b]** *receiving* over the network at the client from the authentication system, an access token that corresponds to the sign-up request, for use at a third[-]party key storage system;
>
> **[c]** *generating* a key by the client; and
>
> **[d]** *sending* over the network from the client to the third[-]party key storage system and by passing the authentication system, one or more messages that include the access token, the key, and a request to encrypt the key.

Id. at 11:62–12:12 (italics and limitation numbering added).

As the italicized language shows, the claim is comprised of several functional steps, each of which describes either communication between systems over a network or generation of a key by the client. A visualization of these functional steps is included below.



First, **[a]** a client (*e.g.*, a user's computer) *sends* a "sign-up request for a user account" to an "authentication system." *Id.* at 12:1–3. In response, **[b]** the client *receives* (from the authentication system) an "access token . . . for use at a third[-]party key storage system." *Id.* at 12:4–7. The client then **[c]** "generat[es] a key." *Id.* at 12:8. And finally, **[e]** the client sends "the access token, the key, and a request to encrypt the key" directly to a "third[-]party key storage system," "bypassing the authentication system." *Id.* at 12:9–12.

Magic's complaint *admits* that it was already well-known for users to **[c]** generate their own keys and **[d]** store them with a third-party key storage provider. D.I. 1 ¶ 27. But it nonetheless alleges that the claims embody a "new system architecture" in which "[t]he software service provider acts as a *non-custodial* intermediary between the end user and the third-party key storage provider." *Id.* ¶ 31.

IV. <u>LEGAL STANDARD</u>

The Supreme Court's *Alice* decision established a two-part framework for determining eligibility under § 101. 573 U.S. at 217–18. First, a court must "look at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter," such as an abstract idea. *Affinity Labs of Tex., LLC v. DirectTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016). If the claim is directed to excluded subject matter, then the Court proceeds to step two and asks whether the claim elements, considered "both individually and 'as an ordered combination[,]' . . . 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (quoting *Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.*, 566 U.S. 66, 78 (2012)). Whether a claim recites patent-eligible subject matter is a question of law that may be resolved by way of a motion to dismiss. *E.g.*, *Content Extraction*, 776 F.3d at 1351. To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). However, a court need not accept "legal conclusions," *id.*, or "allegations that contradict matters properly subject to judicial notice or by exhibit, such as the claims and the patent specification," *Secured Mail Sols. LLC v. Universal Wilde, Inc.*, 873 F.3d 905, 913 (Fed. Cir. 2017) (internal quotation omitted).

V. ARGUMENT

A. *Alice* Step One: The Representative Claim Is Directed To An Abstract Idea.

Claim 11 is directed to the abstract idea of using a software program to facilitate the set up of third-party key storage. But using software to implement a *known* process (*i.e.*, generating keys locally and then sending them to a third-party key storage custodian for encryption) is an abstract idea. *See, e.g.*, *Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1054–56 (Fed. Cir. 2017) (claims using software to implement a "previously manual" process, specifically manual processing of loan applications, were directed to the abstract idea of the "known process," namely, the idea of processing loan applications).

As explained above (at 3–4), claim 11 is comprised of four functional steps, geared towards facilitating the set up of third-party key storage. Two of these steps, **[c]** generating a key and **[d]** sending a key to a third-party HSM for encryption and storage, are *directly* within the scope of admitted prior art. *See* D.I. 1 ¶ 27. The only thing claim 11 adds is the idea of having an "authentication system" *facilitate* that process by providing an "access token." '321 patent, 12:1–12. More specifically, the claim includes two steps, **[a]** and **[b]**, which call for an "authentication system" to provide the client with an "access token" that is, in step **[d]**, passed on to the third-party key storage provider. *Id.* According to the specification's very brief discussion of the token, this "access token" simply facilitates access; it allows the client "to directly communicate with" a third-party key storage provider. *Id.* at 4:50–55; *but see ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 766 (Fed. Cir. 2019) (noting that "while the specification may help illuminate the true focus of a claim, when analyzing patent eligibility, reliance on the specification must always yield to the claim language in identifying that focus."). The focus of the claims as a whole is therefore facilitating the set up of third-party key storage.

Magic's complaint confirms that the "focus of the claimed advance" is the idea of facilitating the set up of third-party key storage. The complaint emphasizes that the advance was not just third-party key storage—using third-party HSMs was already a conventional approach—but more specifically having the software facilitate the set up process. As the complaint puts it, the software "acts as a *non-custodial* intermediary between the end user and the third-party key storage provider, providing the infrastructure the user needs to securely generate keys and coordinate with a third-party key storage provider," without sacrificing the user's control over her keys. D.I. 1 ¶ 31 (italics in original); *Id.* ¶ 30 (saying the claimed solution offers "convenience"). Magic's allegations therefore make clear that the concept at the heart of the '321 patent is using software to facilitate the key generation and management process that the user would otherwise have to figure out themselves. The only difference between the prior art third-party key storage method, *see* D.I. 1 ¶ 27, and what is described in the '321 patent is that the claimed process uses software to facilitate the process from the end user's perspective. Accordingly, the "focus of the claimed advance" is facilitating the set up of third-party key storage.

1. <u>Software Facilitation Of A Known Process Is An Abstract Idea.</u>

Courts consistently find claims directed to software facilitation of a known process (including, specifically, setting up third-party storage) to be abstract and ineligible. In *Alice*, the foundation of modern patent-eligibility jurisprudence, the Supreme Court found that patent claims "designed to facilitate the exchange of financial obligations between two parties by using a computer system as a third-party intermediary" were directed to an abstract idea. 573 U.S. at 213, 218. In particular, the Supreme Court found that the claims were drawn to the fundamental, long prevalent "concept of intermediated settlement" because the claimed software simply "issues . . . instructions to the exchange institutions to carry out the permitted transactions." *Id.* at 219–20. Just like the software in *Alice* directed the "exchange institutions" to carry out the abstract idea of escrow, the claims here simply connect the client with a third-party key storage provider (by way of a generic "access token") and direct the client to carry out the long prevalent concept of setting up third-party key storage. *See* D.I. 1 ¶ 27. Simply facilitating a known process is abstract. *See also Broadsoft, Inc. v. CallWave Commc'ns, LLC*, 282 F. Supp. 3d 771, 781 (D. Del. 2017) (claimed system "facilitat[ing] connecting a caller with a called party" was abstract like the claims in *Alice*); *Cloud Satchel, LLC v. Amazon.com, Inc.*, 76 F. Supp. 3d 553, 562–63 (D. Del. 2014) (claims "facilitat[ing]" an abstract idea using "claim language [that] does nothing more than describe the contours of [the idea]" are abstract.).

Magic characterizes the claimed software as an "intermediary" that manages the process of setting up third-party key storage on behalf of the user. D.I. 1 ¶ 31. To the extent a software "intermediary" is any different from "facilitating" the process using software, the claims are still abstract. In *LendingTree, LLC v. Zillow, Inc.*, for instance, the Federal Circuit found that claims reciting a software "intermediary" that coordinated data transmission for processing loan applications were directed to an abstract idea. 656 F. App'x 991, 996 (Fed. Cir. 2016). The Federal Circuit concluded that the fact that "the patents in suit use a [computerized] broker . . . to organize the [loan application] process is of no consequence" because "third-party intermediar[ies]" are "a building block of the modern economy." *Id.*[3] Whether framed as "facilitating" a process using

[3] *See also GoDaddy.com LLC v. RPost Commc'ns Ltd.*, No. CV-14-00126, 2016 WL 3165536, at *9 (D. Ariz. June 7, 2016) ("collecting and providing information about a dispatch using a third party intermediary" was "an abstract idea [with] an extensive history dating back decades, if not centuries"), *aff'd*, 685 F. App'x 992 (Fed. Cir. 2017); *Card Verification Solutions, LLC v. Citigroup Inc.,* No. 13 C 6339, 2014 WL 4922524, at *4 (N.D. Ill. Sept. 29, 2014) ("passing along confidential information through a trusted, third-party intermediary to ensure both that a consumer can complete the transaction and that the necessary confidential information remains secure" was an abstract idea); *EveryMD.com LLC v. Amazon.com, Inc.*, No. CV-17-05573, 2017 WL 6886181, at *7 (C.D. Cal. Dec. 5, 2017), *aff'd*, 737 F. App'x 538 (Fed. Cir. 2018) (similar).

software or using a software "intermediary," claims like those of the '321 patent that replicate a known process using software are directed to an abstract idea.

2. <u>The Claim Merely Recites Generic Data Transmission And Manipulation.</u>

The abstractness of the '321 claims is further confirmed by the fact that the claimed steps are nothing more than generic data transmission and manipulation: "sending," "receiving," "generating," and "sending." '321 patent, 12:1–12. The Federal Circuit and district courts alike have consistently held that claims involving transmitting and manipulating data—including in authentication processes—"fall into a familiar class of claims 'directed to' a patent-ineligible concept." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1352–54 (Fed. Cir. 2016).

In *Electric Power*, for instance, the Federal Circuit held claims directed to "collecting information, analyzing it, and displaying certain results" to be abstract and ineligible. 830 F.3d at 1353. The court explained that data manipulation "by steps people go through in their minds, or by mathematical algorithms," is an abstract idea. *Id.* at 1354. And in *RecogniCorp, LLC v. Nintendo Company*, the Federal Circuit held that claims directed to "encoding and decoding image data" were patent ineligible because "[a] process that started with data, added an algorithm, and ended with a new form of data was directed to an abstract idea." 855 F.3d 1322, 1326–27 (Fed. Cir. 2017). Here, too, the claimed steps are no more than mathematical manipulation of data (in the generating step) and transmitting data (in the others).

Steps **[a]** and **[b]** are simply information transmission between a client (*e.g.*, an end user's computer) and an authentication system. In step **[a]**, the client sends a sign-up request to the authentication system. In step **[b]**, the client receives, from the authentication system, an access token "for use at a third[-]party key storage system" that corresponds to the sign-up request. Thus, steps **[a]** and **[b]** involve nothing more than the transmission of information.

The next parts of the claim, steps **[c]** and **[d]**, merely recite the idea of generating credentials and sending them to a trusted third party for storage. Generating a key, as in step **[c]**, is a standard form of data manipulation that constitutes an abstract idea. Indeed, the claims do not offer further details about how the key is generated, and both the complaint and the specification reflect that key generation is a well-known mathematical process. *See* D.I. 1 ¶¶ 21–23; '321 patent, 5:8–13. In step **[d]**, the client sends the key, along with other data, to the third-party storage system. Like steps **[a]** and **[b]**, this is simply transmitting data. Processes, like that of claim 11, that recite only data transmission and manipulation are generally found abstract. *See, e.g.*, *Smart Sys. Innovations, LLC v. Chi. Transit Auth., Cubic Corp.*, 873 F.3d 1364, 1371–72 (Fed. Cir. 2017) ("acquiring identification data from a bankcard, using the data to verify the validity of the bankcard, and denying access to a transit system if the bankcard is invalid" is directed to the abstract idea of "collection, storage, and recognition of data").

3. __**The Claim Is Not Directed To An Improvement In Computer Functionality.**__

In the context of a computer-implemented invention, courts also assess subject-matter eligibility by asking whether the claims "are directed to an improvement in the functioning of a computer," or merely adding "conventional computer components to well-known business practices." *Affinity Labs*, 838 F.3d at 1260 (internal quotations omitted). To be patent eligible, claims must recite "a specific technical solution . . . to a technological problem." *Universal Secure*, 10 F.4th at 1355. As explained above, claim 11 does not alter the underlying third-party key storage process. It is simply providing for software that facilitates the known process of setting up third-party key storage by connecting users with providers. This may improve the user experience of implementing the abstract idea of third-party storage, but "it is not enough … to merely improve a fundamental practice or abstract process by invoking a computer merely as a tool." *Customedia Techs., LLC v. Dish Network Corp.*, 951 F.3d 1359, 1364 (Fed. Cir. 2020); *Elec. Power*, 830 F.3d at 1354 (claims using "existing computers as tools in aid of processes" are direct to abstract ideas).

That the claims are not directed to an improvement in computer functionality is clear from the functional description of the claims. The claims simply recite high-level functional steps—like "generating" a key and "sending" or "receiving" data over a network—without disclosing any "particular way of programming or designing the software" or "how this would be technologically implemented." *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1241, 1244 (Fed. Cir. 2016). Such "vague, functional" terms, "devoid of technical explanation as to how to implement the invention," are abstract. *In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 615 (Fed. Cir. 2016).

The Federal Circuit addressed a similar situation in *Universal Secure*, which held abstract and ineligible claims directed to "a method for enabling a transaction between a user and a merchant, where the merchant is given a time-varying code instead of the user's secure (credit card) information." 10 F.4th at 1349. The Court found that "the claims 'simply recite conventional actions in a generic way' (e.g., receiving a transaction request, verifying the identity of a customer and merchant, allowing a transaction) and 'do not purport to improve any underlying technology.'" *Id.* (citation omitted). In the same way, claim 11 merely recites conventional actions in a generic way—sending a sign-up request, receiving an access token, generating a key, and sending the key, token, and an encryption request to a third-party storage provider—without explaining how exactly those processes are achieved or purporting to provide any technological improvement. *See infra* 6; *see also Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017) (claims "providing restricted access to resources" using generic steps—"receiving" user identity, "authenticating" user identity, "authorizing," and "permitting access"—

were abstract). Similarly, in *Free Stream Media Corp. v. Alphonso Inc.*, the Federal Circuit found analogous claims, which "facilitate[d] a communication session" between "devices on the same network," to be directed to an abstract idea. 996 F.3d 1355, 1363–64 (Fed. Cir. 2021). The court specifically found that the claims did "not at all describe how that result is achieved," and, even though the specification provided sparse details as to the underlying mechanisms, because nothing in the claims disclosed how that result was achieved, no "improvement to computer functionality" was demonstrated. *Id.* at 1364–65. Here too, the claims allegedly facilitate the set up of third-party key storage, yet they fail to describe any particular technical way that result is achieved. *See supra* 9.

Moreover, nothing in the '321 patent specification "suggests that the [computer system] itself is improved from a technical perspective, or that it would operate differently than it otherwise could." *ChargePoint*, 920 F.3d at 768; *see also Rady v. Boston Consulting Grp.*, 20-cv-02285, 2022 WL 976877, at *3 (S.D.N.Y. Mar. 31, 2022) (no improvement to "the functionality of storing and processing data on a blockchain" when the patent failed to "describe how the patent improves blockchains"). Instead, the specification describes the software in purely functional terms and makes clear that the claims are performed with generic computer components, behaving as usual. *See infra* 14–16 (discussing that the patent claims use only generic computer hardware to perform conventional functional steps).

Rather than improve a technical problem, both the specification and the complaint make clear that the patent is solving a *user experience* problem. *See* '321 patent, 3:34–36 ("[C]onsumer deployment of cryptography-based security has failed to provide an acceptable user experience."); D.I. 1 ¶ 31 (alleging that the patent improves user experience by "providing the infrastructure" needed to delegate the tasks of key generation and storage). The patent solves this user experience issue by facilitating the tasks of setting up third-party key storage, so a user does not need to figure out how to generate keys and coordinate with a third-party key storage provider by herself. *Id.* Merely "improving a user's experience while using a computer application is not, without more, sufficient to render the claims directed to an improvement in computer functionality." *Customedia Techs.,* 951 F.3d at 1365 (collecting cases).[4]

The specification and complaint also indicate the software functions as a "non-custodial intermediary" without access to the user's keys, thereby providing improved security. *See* '321 patent, 1:41–55; D.I. 1 ¶ 31 (italics removed). But this is not an improvement in computer functionality because, as Magic admits, having a user generate keys locally and then store them with a third-party key storage system was well known prior to the '321 patent. D.I. 1 ¶ 27. Adding a software intermediary to facilitate the known process does not add to the expected security already inherent to the known third-party key storage process. *See Universal Secure*, 10 F.4th at 1350–53 (holding that software claims combining two security techniques but achieving nothing "more than the expected sum of the security provided by each technique" ineligible). Much like how the escrow component of the software-implemented escrow in *Alice* was responsible for any mitigation of risk, here, any security provided by the claimed system stems from the well-established process of using a third-party for key storage—not from the addition of software facilitation. 573 U.S. at 220; *see also Universal Secure*, 10 F.4th at 1350 (finding software claims for third-party storage of "secure (credit card) information" abstract and ineligible); *Boom!*

[4] The specification also describes the '321 patent as improving user identity management by increasing security through "a decentralized identifier token (DIDT)."" '321 patent, 3:41–47; *see also id.* at 1:67–2:22, 3:11–13, 3:43–45, 9:10–28 (describing DIDT). None of the patent claims involve this decentralized identifier token. Similarly, the claims do not include any of the steps described in the specification as allowing lost identity recovery. *See id.* at 5:24–28. These purported technological advancements are therefore irrelevant to the § 101 inquiry.

Payments, Inc. v. Stripe, Inc., 839 F. App'x 528, 532 (Fed. Cir. 2021) (explaining that having an intermediary store sensitive payment information—in a word, escrow—is a classic abstract idea, much like the claims found invalid in *Alice*).

In short, the '321 claims are directed to facilitating the set up of third-party key storage. Analogizing to other "facilitation" claims, observing the claims' functional focus on data manipulation and transmission, and examining the claims for any claimed technological improvement all confirm that this is abstract concept under *Alice* step one.

B. *Alice* Step Two: The Claim Includes No Inventive Concept

The '321 patent's claims also fail to provide any "inventive concept" that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [abstract idea] itself." *Alice*, 573 U.S. at 217–18. The Federal Circuit and the Supreme Court have set out two clear rules for what qualifies as an inventive concept. First, "[t]he abstract idea itself cannot supply the inventive concept, 'no matter how groundbreaking the advance.'" *Trading Techs. Int'l, Inc. v. IBG, LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) (citation omitted). Second, elements that are "well-understood, routine, conventional," or "purely functional" cannot "transform" an abstract idea into a patent-eligible application of the idea. *Alice*, 573 U.S. at 225–26 (citation omitted). The '321 patent fails for both reasons; it recites only the abstract idea of facilitating set up of third-party key storage and does so using only conventional, functional elements.

As an initial matter, the patent claims include only generic computer hardware, namely "[a] non-transitory computer readable storage medium," "a program," "a processor," and "a network." '321 patent, 11:62–12:12; *see, e.g.*, *Intellectual Ventures I LLC v. Erie Indem. Co.*, 850 F.3d 1315, 1341 (Fed. Cir. 2017) (a "processor" is generic); *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324 (Fed. Cir. 2016) (a "network" is generic); *GeoComply Sols. v. Xpoint Servs.*, No. 22-1273, 2023 WL 1927393, at *8 (D. Del. Feb. 10, 2023) (similar). The specification likewise makes clear that the invention requires only generic computer hardware. *See* '321 patent, 10:43–47 (describing the "components contained in the computer system" as "those typically found in computer systems"). "[G]eneric computer components [are] insufficient to add an inventive concept to an otherwise abstract idea." *TLI*, 823 F.3d at 614.

Nor is there an inventive concept in any of the individual functional steps: "sending a sign-up request"; "receiving . . . an access token"; "generating a key"; and "sending . . . the access token, the key, and a request to encrypt the key." '321 patent, 12:1–12. The recited components "behave exactly as expected according to their ordinary use" and therefore cannot confer patent eligibility. *TLI*, 823 F.3d at 615.

To start, nothing in the claims or the specification differentiates "a sign-up request for a user account with the decentralized application" from any other sign-up request for a user account. '321 patent, 12:1–3. Similarly, the patent offers no indication that the claimed "access token" is anything other than conventional. Claim 11 offers no particulars regarding the token, specifying only that that the access token "corresponds with the sign-up request" and is "for use at a third[-]party key storage server." *Id.* at 12:5–7. The specification's similarly sparse description provides:

> The time bound access token may include time-to-live (TTL) data embedded within the token. . . . The time bound token allows client . . . to directly communicate with third party service.

Id. at 4:49–55. In short, the access token simply appears to be a token—a piece of data—that allows the client to communicate with the third-party key storage provider. Courts have routinely rejected such generic tokens as inventive concepts. In *Universal Secure*, for instance, the claimed system involved transmitting a "time-varying code" that could be used "to access a database" and to allow "a third party or credit card company to approve . . . the transaction." 10 F.4th at 1349. The Federal Circuit explained that use of such codes is "conventional and long-standing," and therefore cannot constitute an inventive concept. *Id.* at 1350. The generic access token here is functionally equivalent to the time-varying codes in *Universal Secure*. *See also Asghari-Kamrani v. United Servs. Auto. Ass'n,* No. 15-cv-478, 2016 WL 3670804, at *1 (E.D. Va. July 5, 2016), *aff'd*, 737 F. App'x 542 (Fed. Cir. 2018) (using a time-dependent code for authentication did not constitute an inventive concept). Alternately, the token is similar to other conventional access-granting elements, like a ticket or wristband; nothing in the '321 patent—and certainly nothing in the claims— indicates that access tokens are anything other than conventional. *See Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1149 (Fed. Cir. 2016) (explaining that an inventive concept must be captured in the claims); *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1345 (Fed. Cir. 2013) ("[D]etail in the specification does not transform . . . an abstract concept into a patent-eligible system").

In the same vein, the claimed key generation process is no different from conventional key generation. The specification makes clear that key generation is a known cryptographic process (that is, math) that was not invented by the '321 patent. *See* '321 patent, 5:8–12. And Magic's own complaint confirms that, prior to the '321 patent, end users would generate keys and then store them with prior art third-party HSMs—so the "non-custodial" aspect of the key generation described in claim 11 (*i.e.*, the client generating the key) was likewise conventional. D.I. 1 ¶ 27.

Lastly, there is no indication that the final step of the claim, "sending . . . the access token, the key, and a request to encrypt the key" differed in any way from conventional network-based communication. '321 patent, 12:9–12.

In sum, none of the claimed steps involve anything beyond using conventional computer components as they were designed to be used, and the use of conventional components for their conventional purposes cannot constitute an inventive concept that confers patent eligibility. *See,* *e.g.*, *TLI*, 823 F.3d at 613 ("[C]omponents must involve more than performance of 'well-understood, routine, conventional activities' previously known to the industry' . . . to add an inventive concept sufficient to bring the abstract idea into the realm of patentability." (quoting *Alice*, 573 U.S. at 225)). Instead, as explained above, they recite an abstract, facilitation of using third-party key storage and require that it be implemented in the blockchain context.

Magic's complaint suggests that—even if the individual steps are conventional—the Court should nonetheless find an inventive concept because the steps collectively provide for a "new system architecture that inverted the conventional industry architectures." D.I. 1 ¶ 31; *see BASCOM Glob. Internet Servs. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016) (holding that a claim's "particular arrangement of elements" constituted an inventive concept). Specifically, Magic alleges that the architecture was "new" because it does not rely on "one entity (either the end user or a software service provider) [to] manage key generation and storage," but rather splits them across the end user, a software service provider, and a third-party key storage system. D.I. 1 ¶ 31. But this supposedly inventive architecture is nothing but the abstract idea itself—having a software intermediary facilitate the set up of third-party key storage—and therefore cannot constitute an inventive concept. *BASCOM* , 827 F.3d at 1349 ("An inventive concept that transforms the abstract idea into a patent-eligible invention must be significantly more than the abstract idea itself . . . ."). The Federal Circuit reached the same conclusion regarding the intermediary in *Universal Secure*, which supposedly constituted a new architecture that would "mitigate information security risks." *Universal Secure*, 10 F.4th at 1350. "Because sending data to a third-party as opposed to the merchant is itself an abstract idea," the Court explained, "it cannot serve as an inventive concept." *Id.* So too here.

Moreover, Magic's own complaint acknowledges that the idea of having a third party store a user-generated key was well understood in the art prior to the '321 patent. D.I. 1 ¶ 27. In these "[t]hird-party HSMs"—as in claim 11—the end user would "generat[e] keys and coordinat[e] with the third-party provider" to store and encrypt those keys. *Id*. The only thing the '321 patent adds is having software facilitate that process—and there is nothing inventive about having a software intermediary facilitate the same steps used in the prior art.

This case is therefore unlike *BASCOM*, where the "non-conventional and non-generic arrangement of known, conventional pieces" allowed for new technical capabilities, and therefore constituted an inventive concept. *See BASCOM*, 827 F.3d at 1350 (Fed. Cir. 2016). In reaching this finding, the Federal Circuit noted that the claims did not "preempt all ways of" achieving the abstract idea to which they were directed, and "the patent describe[d] how its particular arrangement of elements [was] a technical improvement over prior art ways." *Id.* Here, the software is simply facilitating the process of client-based key generation and coordination with a third-party key storage system that would otherwise have to be performed by an end user. That may be valuable from a user experience perspective, but the technical capabilities of the system—at least as claimed—are the exact same as the prior art third-party key storage systems.

C. <u>The Remaining Claims Are Similarly Ineligible.</u>

Claim 11 is the only claim specifically asserted (or even referenced) in the complaint. *See* D.I 1 ¶¶ 36–61. To the extent Magic disputes the representativeness of claim 11, however, there is no doubt that the additional claims of the '321 patent are directed to the same abstract idea and include no inventive concept.

- Claims 1 and 21 merely restate Claim 11 as a method claim and system claim, respectively. '321 patent, 11:5–19, 12:59–13:9. Neither adds content relevant to § 101.

- Claims 2–5 and 12–15 recite additional generic details regarding the sending and receiving of the initial sign-up request, including "sending first authentication information over the network," *id.* at 11:20–23, 12:13–16; "receiving the request for first authentication information over the network," *id.* at 11:24–27, 12:17–20; having that request involve "an email at the client" or "a message at a phone number associated with the client," *id.* at 11:28–34, 12:21–28; and having the sign up request "include[] sending a login request," *id.* at 11:35–37, 12:29–32. Invoking additional generic computer elements and data transmission does not change the § 101 analysis. *Intellectual Ventures I*, 850 F.3d at 1329 ("sending and receiving information" are "routine computer functions"); *supra* 14–16.
- Claims 6 and 16 specify that the "key" generated by the client is a "public-private key pair." '321 patent, 11:38–40, 12:33–35. But as the specification makes clear and Magic's complaint concedes, private-public key pairs were well understood and conventional prior to the '321 patent (and, indeed, prior to the invention of blockchain). *Id.* at 3:32–40; D.I. 1 ¶¶ 21–23; *see Bancorp Servs., LLC v. Sun Life Assur. Co. of Can.*, 687 F.3d 1266, 1274 (Fed. Cir. 2012) (appending well-known computer components does not "salvage an otherwise patent-ineligible process"); *supra* 14–18.
- Claims 7 and 17 provide that the access token received at the client from the authentication system was "generated at the third-party key storage server." '321 patent, 11:41–44, 12:36–40. Specifying where the access token is generated does not change the focus of the claims, especially given that it provides no further detail about what the token is or does. *Supra* 9–11.
- Claims 8 and 18 recite that the client sends an "authentication credential" to the third-party key storage server. '321 patent, 11:45–50, 12:41–46. Claims 9 and 19 provide that the "authentication credential" is received. *Id.* at 11:51–53, 12:47–49. Here too, adding steps of

sending and receiving credentials using generic network communication does not change the § 101 analysis. *See buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014); *supra* 8–10.

- Claims 10 and 20 provide that the information sent from the client to the third-party key storage server goes in a specific order: first the access token, followed by the authentication credential, the key, and the request to encrypt the key. ’321 patent, 11:54–61, 12:50–58. This is purely the sending of information between the client and the third-party key storage server. And nothing in the patent suggests that anything about this order is unconventional: the access token allows the client "to directly communicate" with the third-party key storage server, so it makes sense to be sent before the rest of the information. *Id.* at 4:54–55; *see supra* 8–10.

In sum, the other claims, like representative claim 11, are directed to the abstract idea of facilitating set up of third-party key storage. They do not change the focus of the claims, do not recite any inventive concepts, and therefore do not change the patent eligibility calculus.

VI. <u>CONCLUSION</u>

Privy respectfully requests that the Court grant its motion and hold the ’321 patent invalid under § 101. Privy further requests that the Court dismiss *with prejudice*. Magic’s complaint already attempts to plead around subject-matter ineligibility. Dismissal without leave to amend is proper where, as here, there is no chance that further allegations would change the outcome. *See Fast 101 Pty Ltd. v. Citigroup Inc.*, 424 F. Supp. 3d 385, 393 (D. Del. 2020) (dismissing under § 101 without leave to amend).

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jack B. Blumenfeld

Jack B. Blumenfeld (#1014)
Brian P. Egan (#6227)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
jblumenfeld@morrisnichols.com
began@morrisnichols.com

Attorneys for Defendant

OF COUNSEL:

Clement S. Roberts
ORRICK, HERRINGTON
& SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

Alyssa Caridis
ORRICK, HERRINGTON
& SUTCLIFFE LLP
355 South Grand Avenue, Suite 2700
Los Angeles, CA 90071
(213) 629-2020

November 16, 2023

CERTIFICATE OF SERVICE

I hereby certify that on November 16, 2023, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on November 16, 2023, upon the following in the manner indicated:

Daniel M. Silver, Esquire *VIA ELECTRONIC MAIL*
Alexandra M. Joyce, Esquire
MCCARTER & ENGLISH, LLP
Renaissance Centre
405 North King Street, 8th Floor
Wilmington, DE 19801
Attorneys for Plaintiff

Daralyn J. Durie, Esquire *VIA ELECTRONIC MAIL*
Ragesh K. Tangri, Esquire
Timothy C. Saulsbury, Esquire
Michael Burshteyn, Esquire
Joyce C. Li, Esquire
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105
Attorneys for Plaintiff

Sara Doudar, Esquire *VIA ELECTRONIC MAIL*
MORRISON & FOERSTER LLP
707 Wilshire Blvd.
Los Angeles, CA 90017
Attorneys for Plaintiff

/s/ Jack B. Blumenfeld

Jack B. Blumenfeld (#1014)